IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	: Godwin et al.
Serial No.	: 09/764,252
Filed	: January 17, 2001
Title	: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR PROVIDING DATA FROM NETWORK SECURE COMMUNICATIONS IN A CLUSTER COMPUTING ENVIRONMENT
Attorney Docket	: 5577-220 (IBM018PA)
Examiner	: A. Patel
Art Unit	: 2154
Confirmation	: 8043

MS Issue Fee
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Interview Summary

This paper is being filed in response to an Examiner Initiated telephone Interview dated September 20, 2007, in the identified application.

Statement of the Substance of the Interview begins on page 2 of this paper.

Statement Of The Substance Of The Interview

On September 20, 2007, Thomas Lees on behalf of the applicants conducted an Examiner-initiated telephone interview with Examiner Patel. Thanks to the Examiner once again, for his time and consideration during the telephone interview. No demonstrations were utilized. Additionally, no exhibits were transmitted to the Examiner. During the interview, the Examiner identified a new reference, U.S. Pat. No. 6,463,475 to Calhoun (hereinafter, '*Calhoun*'), which was not cited or considered in the previous prosecution and was first brought to the applicants' attention during this interview. The claims were not discussed in detail at the time of the initial telephone call from the Examiner as the applicants wanted time to review and study the newly identified reference.

On September 24, 2007, the applicants transmitted to the Examiner, an unofficial proposed amendment to claim 1 via electronic mail.

On September 25, 2007, Examiner Patel telephoned Thomas Lees and requested to see unofficial proposed changes to the remainder of the independent claims (20 and 39) that were analogous to the proposed changes to claim 1 e-mailed to the Examiner on September 24, 2007.

After communicating additional proposed claim amendments to the Examiner, Thomas Lees, on behalf of the applicants, telephoned Examiner Patel and authorized him to cancel the systems and computer program product claims. The applicants further indicated that such canceled claims would be prosecuted in a subsequently filed continuation application.

The claim amendments and cancellations in the proposed amendments of September 24, 25, were made for the purpose of facilitating expeditious prosecution of allowable subject matter. The applicants do not concede that the claims pending prior to the above amendments define unpatentable subject matter over the references cited by the Examiner, including the newly cited

Calhoun reference, and further reserve the right to pursue additional claims in one or more continuing applications.

Copies of all Internet e-mail correspondence are provided in the attachments included with this paper including:

4 page e-mail correspondence including unofficial proposed amendments to claims 1, 20 and 39 from Thomas Lees to Examiner Patel, September 25, 2007.

4 page e-mail correspondence including unofficial proposed amendment to claim 1 and general comments from Thomas Lees to Examiner Patel, September 24, 2007.

The general thrust of the principal arguments of Examiner Patel can be seen, for example, in Figs. 2 and 7 of *Calhoun* and the corresponding descriptions in the associated specification. The general thrust of the principal arguments of the applicants is at least substantially as set out in the comments provided in the e-mail from the applicants to the Examiner dated Sept. 24, 2007.

No other pertinent matters were discussed and no conclusions were reached.

Respectfully submitted,
Stevens & Showalter, L.L.P.
By /Thomas E. Lees/
Thomas E. Lees Reg. No. 46,867

7019 Corporate Way
Dayton, Ohio 45459-4238
Telephone: 937-438-6848
Facsimile: 937-438-2124
Email: tlees@sspatlaw.com

October 19, 2007

Tom Lees

From: Tom Lees [tlees@sspatlaw.com]
Sent: Tuesday, September 25, 2007 10:20 AM
To: 'ashok.patel3@uspto.gov'
Subject: Unofficial communication regarding Application serial no. 09/764252

Examiner Patel:

Thank you for the telephone call this morning. Per your request, please find below, the changes per our earlier discussions for each of the independent claims, 1, 20 and 39. Claims 20 and 39 have been amended in a manner analogous to amended claim 1.

1. (Currently Amended) A method for providing secure communications over a network in a distributed workload environment having target hosts which are accessed through a distribution processor by a common network address, the method comprising the steps of:

receiving at the distribution processor, network communications directed to the common network address;

determining whether the network communications are secure network communications;

processing secure network communications by:

routing both inbound and outbound communications with target hosts which are associated with an end-to-end secure network communication through the distribution processor;

processing both inbound and outbound end-to-end secure network communications at the distribution processor so as to provide endpoint network security processing of communications from the target host to the distribution processor and endpoint network security processing of communications from the distribution processor to the target host such that the distribution processor serves as an endpoint for the end-to-end secure network communication; and

~~receiving at the distribution processor, network communications directed to the common network address;~~

distributing the received secure network communications that are directed to the common network address among selected ones of the target hosts so as to distribute workload associated with the network communications among the target hosts including encapsulating communications between the distribution processor and the selected ones of the plurality of target hosts which are associated with end-to-end secure network communications so as to distinguish communications between the distribution processor and the selected ones of the plurality of target hosts which are associated with secure network communications from other communications; and

processing non-secure communications by distributing the received network communications that are directed to the common network address among ~~selected ones of~~ the target hosts~~, wherein the selection among the target hosts is carried out~~ so as to distribute workload associated with the network

communications among the target hosts.

20. (Currently Amended) A system for providing secure communications over a network in a distributed workload environment having target hosts associated with a common IP address and which are accessed through a distribution processor by a common network address, comprising:

means for receiving at the distribution processor, network communications directed to the common network address;

means for determining whether the network communications are secure network communications;

means for processing secure network communications having:

means for routing both inbound and outbound communications with target hosts which are associated with an end-to-end secure network communication through the distribution processor;

means for processing both inbound and outbound end-to-end secure network communications at the distribution processor so as to provide endpoint network security processing of communications from the target host to the distribution processor and endpoint network security processing of communications from the distribution processor to the target host such that the distribution processor serves as an endpoint for the end-to-end secure network communication; and

~~means for receiving at the distribution processor, network communications directed to the common network address;~~

means for distributing the received secure network communications that are directed to the common network address among selected ones of the target hosts so as to distribute workload associated with the network communications among the target hosts including means for encapsulating communications between the distribution processor and the selected ones of the plurality of target hosts which are associated with end-to-end secure network communications so as to distinguish communications between the distribution processor and the selected ones of the plurality of target hosts which are associated with secure network communications from other communications; and

means for processing non-secure communications by distributing the received network communications that are directed common network address among ~~selected ones of~~ the target hosts~~, wherein the selection among the target hosts is carried out~~ so as to distribute workload associated with the network communications among the target hosts.

39. (Currently Amended) A computer program product for providing secure communications over a network in a distributed workload environment having target hosts associated with a common IF address and which are accessed through a distribution processor by a common network address, comprising:

a computer readable medium having computer readable program code embodied therein, the computer readable program code comprising:

computer readable program code which receives at the distribution processor, network communications directed to the common network address;

computer readable program code which determines whether the network communications are secure network communications;

computer readable program code which processes secure network communications including:

computer readable program code which routes both inbound and outbound communications with target hosts which are associated with an end-to-end secure network communication through the distribution processor;

computer readable program code which processes both inbound and outbound end-to-end secure network communications at the distribution processor so as to provide endpoint network security processing of communications from the target host to the distribution processor and network security processing of communications from the distribution processor to the target host such that the distribution processor serves as an endpoint for the end-to-end secure network communication; and

~~computer readable program code which receives at the distribution processor, network communications directed to the common network address;~~

computer readable code which distributes the received secure network communications that are directed to the common network address among selected ones of the target hosts so as to distribute workload associated with the network communications among the target hosts including computer readable program code which encapsulates communications between the distribution processor and the selected ones of the plurality of target hosts which are associated with end-to-end secure network communications so as to distinguish communications between the distribution processor and the selected ones of the plurality of target hosts which are associated with secure network communications from other communications; and

computer readable program code which processes non-secure communications by distributing ~~distributes~~ the received network communications that are directed to the common network address among ~~selected ones of~~ the target hosts~~, wherein the selection among the target hosts is carried out~~ so as to distribute workload associated with the network communications among the target hosts.

If you would like me to submit a formal amendment or listing of claims, please let me know.

Best regards

Tom Lees

Thomas E. Lees
Stevens & Showalter, L.L.P.
7019 Corporate Way
Dayton, OH 45459-4238
Phone: (937)438-6848
Fax: (937)438-2124
E-mail: tlees@sspatlaw.com
Web: www.sspatlaw.com

Tom Lees

From: Tom Lees [tlees@sspatlaw.com]
Sent: Monday, September 24, 2007 2:44 PM
To: 'ashok.patel3@uspto.gov'
Subject: Unofficial communication regarding Application serial no. 09/764252

Examiner Patel:
Per your request, below is an unofficial proposed claim amendment to claim 1, along with comments, and citation to support for the changes in the specification.

Please feel free to call or email with suggestions or comments.

Best regards

Tom Lees

1. (Currently Amended) A method for providing secure communications over a network in a distributed workload environment having target hosts which are accessed through a distribution processor by a common network address, the method comprising the steps of:

receiving at the distribution processor, network communications directed to the common network address;

determining whether the network communications are secure network communications;

processing secure network communications by:

routing both inbound and outbound communications with target hosts which are associated with an end-to-end secure network communication through the distribution processor;

processing both inbound and outbound end-to-end secure network communications at the distribution processor so as to provide endpoint network security processing of communications from the target host to the distribution processor and endpoint network security processing of communications from the distribution processor to the target host such that the distribution processor serves as an endpoint for the end-to-end secure network communication; and

~~receiving at the distribution processor, network communications directed to the common network address;~~

distributing the received secure network communications that are directed to the common network address among selected ones of the target hosts so as to distribute workload associated with the network communications among the target hosts including encapsulating communications between the distribution processor and the selected ones of the plurality of target hosts which are associated with end-to-end secure network communications so as to distinguish communications between the distribution processor and the selected ones of the

plurality of target hosts which are associated with secure network communications from other communications; and

processing non-secure communications by distributing the received network communications that are directed to the common network address among ~~selected ones of~~ the target hosts~~, wherein the selection among the target hosts is carried out~~ so as to distribute workload associated with the network communications among the target hosts.

Comments:

1. I merely moved the "receiving" step up to the front for clarity

Support for the proposed new "determining" and "processing" steps can be found, for example, in Fig. 5A and paragraphs 71, 80 of applicant's US2002/0095603.

Support for the amendments to the encapsulation step can be found for example, in Fig. 5A and paragraph 83 of applicant's US2002/0095603.

Brief comments with regard to US 6,463,475 to Calhoun, (hereinafter "*Calhoun*").

Calhoun provides a tunnel switch that combines load balancing and L2TP tunnel mapping.

However, *Calhoun* fails to teach or suggest:

> processing both inbound and outbound end-to-end secure network communications at the distribution processor so as to provide endpoint network security processing of communications from the target host to the common network address and endpoint network security processing of communications from the distribution processor to the target host such that the distribution processor serves as an endpoint for the end-to-end secure network communication....

The L2TP tunnels described in *Calhoun* are *per se*, not secure. This can be seen because there is a lack of confidentiality that is inherent in the L2TP protocol. In this regard, the disclosed tunnels merely allow packets of one network to be transported over another network.

For example, the tunnel switch 100 attempts to address this inherent lack of security by utilizing authentication (see Col 5, lines 43-48) to verify that the user originating the tunnel has the appropriate permission to access the destination. However, verifying the authenticity of a user fails to teach or suggest providing endpoint network security processing of communications. Moreover, there is at least no endpoint security processing of communications from the tunnel switch to the client back. See also Fig. 7 and para. 8, lines 6-35, which outlines the method of authentication of the user to the destination. Regardless of any authentication processes, no security processing is provided for returned information.

Further, *Calhoun* fails to teach or suggest:

> ... encapsulating communications between the distribution processor and the selected ones of the plurality of target hosts which are associated with end-to-end secure network communications so as to distinguish communications between the distribution processor and the selected ones of the plurality of target hosts which are associated with secure network communications from other communications ... processing non-secure communications by distributing the received network communications that are directed to the common network address among...

The encapsulation using L2TP in *Calhoun* is used explicitly to map incoming tunnels to corresponding outgoing tunnels, e.g., as determined by the dispatch process 130. See Col. 5, lines 48-63. In *Calhoun*, every received packet in the tunnel 50 that is associated with a switched tunnel is re-encapsulated with the information corresponding to the associated switched tunnel 52 as a manner of routing the packet. That is, in *Calhoun*, encapsulating is the way to identify the destination address.in L2TP. As such, there is no way to distinguish secure communications from non-secure communications in either the incoming tunnel 50 or in any of the switched tunnels 52. As noted above, no packets are treated as secure communications. Rather, the only security is on a user level (via authentication – compared to packet level security where specific packets are considered secure communications).

Thomas E. Lees
Stevens & Showalter, L.L.P.
7019 Corporate Way
Dayton, OH 45459-4238
Phone: (937)438-6848
Fax: (937)438-2124
E-mail: tlees@sspatlaw.com
Web: www.sspatlaw.com